

AMENDMENTS TO THE SPECIFICATION

Page 22, paragraph [0037]:

Figures 1-3 illustrate certain aspects of the facility. Figure 1 is a high-level block diagram showing a typical environment in which the facility operates. The block diagram shows several voter computer systems 110, each of which may be used by a voter to submit a ballot and verify its uncorrupted receipt. Each of the voter computer systems are connected via the Internet 120 to a vote collection center computer system 150_130. Those skilled in the art will recognize that voter computer systems could be connected to the vote collection center computer system by networks other than the Internet, however. The facility transmits ballots from the voter computer systems to the vote collection center computer system, which returns an encrypted vote confirmation. In each voter computer system, the facility uses this encrypted vote confirmation to determine whether the submitted ballot has been corrupted. While preferred embodiments are described in terms in the environment described above, those skilled in the art will appreciate that the facility may be implemented in a variety of other environments including a single, monolithic computer system, as well as various other combinations of computer systems or similar devices connected in various ways.

Page 23, paragraph [0040]:

In step 301, on the voter computer system, the facility encodes a ballot choice selected by the voter in order to form a ballot. In step 302, the facility encrypts this ballot. In some embodiments, the encrypted ballot is an ElGamal pair, generated using an election public key and a secret maintained on the voter computer system. In step 303, the facility optionally signs the ballot with a private key belonging to the voter. In step 304, the facility constructs a validity proof that demonstrates that the encrypted ballot is the encryption of a ballot in which a valid ballot choice is selected. In step 305, the facility transmits the encrypted, signed ballot and the validity proof 311 to a vote collection center computer system.